FREEDMAN + TAITELMAN, LLP
MICHAEL A. TAITELMAN (SBN 151990)
mtaitelman@ftllp.com
JESSE KAPLAN (SBN 255059)
jkaplan@ftllp.com
1901 Avenue of the Stars, Suite 500
Los Angeles, California 90067
Tel.: (310) 201-0005
Fax: (310) 201-0045

Attorneys for Plaintiffs
HIGHPOINT ASSOCIATES, LLC and SUMEET GOEL

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

HIGHPOINT ASSOCIATES , LLC, a California limited liability company, SUMEET GOEL, an individual, Plaintiff, vs. JOHN DOE; and DOES 2 through 10, inclusive, Defendants.	CASE NO. 2:15-cv-00497 FMO(JPRx) DISCOVERY MOTION **PLAINTIFFS' MOTION FOR EXPEDITED DISCOVERY TO IDENTIFY THE DOE DEFENDANTS** Date: March 26, 2015 Time: 10:00 a.m. Courtroom: A - 8th Floor Honorbale Jean P. Rosenbluth

PLEASE TAKE NOTICE THAT, Plaintiffs Highpoint Associates, LLC ("HPA") and Sumeet Goel ("Goel") (collectively, "Plaintiffs"), will move this honorable Court on March 26, 2015 at 10:00 a.m, at the United States District Court for the Central District of California, located at 312 N. Spring St., Los Angeles, CA 90012, Courtroom A – 8th Floor, before the Honorable Jean P. Rosenbluth, for an Order allowing Plaintiffs to obtain limited expedited discovery from third Parties prior to conducting a meeting between the parties pursuant to F.R.C.P 26(f).

Specifically, Plaintiffs seek to serve subpoenas on Microsoft ("Microsoft"), Bullhorn, Inc. ("Bullhorn") and London Trust Media ("LTM"). The contemplated subpoenas would seek the production of documents that would identify the Doe defendants herein. Good cause exists to allow Plaintiffs to obtain this discovery because the Doe defendants in this matter have cloaked their identity using anonymous IP addresses to access Plaintiffs various electronic communications and other information. Without subpoenas requiring LTM, Bullhorn and Microsoft to provide Plaintiffs with information identifying the persons illegally accessing Plaintiffs' electronic communications and other information, Plaintiffs cannot identify the defendants and prosecute this lawsuit.

As there are no known defendants in this matter, Plaintiffs' counsel was unable to meet and confer with any party pursuant to L.R. 7-3.

DATED: February 6, 2015

FREEDMAN + TAITLEMAN, LLP

By: /s/
MICHAEL A. TAITELMAN
JESSE KAPLAN
Attorneys for Plaintiffs HIGHPOINT ASSOCIATES, LLC and SUMEET GOEL

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs Highpoint Associates, LLC ("HPA") and its founder and sole member, Sumeet Goel ("Goel") (collectively, "Plaintiffs"), must identify the Doe defendants using anonymous IP addresses to access various electronic communications and other information of Plaintiffs. Unfortunately, because these IP addresses are anonymous, Plaintiffs are unable to ascertain the identity of these anonymous defendants (”Defendants”).

Accordingly, Plaintiffs seek leave of Court to serve certain limited expedited discovery on Microsoft ("Microsoft"), Bullhorn, Inc. ("Bullhorn") and London Trust Media ("LTM") that will likely reveal Defendants' identity. Specifically, Plaintiffs seek to serve a subpoena on Microsoft (for all HPA related access including dates, times, IP addresses, etc., by username). These logs for accessing HPA emails are hosted in the cloud using the Microsoft service called "Office365" and Plaintiffs were advised a subpoena is required to release the entirety of the requested documents. Additionally, Plaintiffs seek to serve subpoenas on Bullhorn and LTM to determine the source of unauthorized access to Plaintiffs accounts using anonymous IP addresses. (Declaration of Jesse Kaplan, "Kaplan Decl." ¶3; Declaration of Sumeet Goel "Goel Decl." ¶2)

II. BACKGROUND.

A. Plaintiffs Confidential Account Information.

Founded in 2002 by Goel, HPA is a consulting company providing interim executive resources, from its network of carefully vetted and highly qualified professionals, to its global clients ranging from small and mid-sized businesses to Fortune 100 corporations, and investment firms. (Goel Decl., ¶3)

HPA maintains its proprietary and confidential client and consultant information, along with other business related information, on its internal network as well as on third party database management systems and email hosting server systems. HPA emails are hosted in the cloud through a Microsoft service called "Office365". (Goel Decl., ¶4)

HPA also conducts its business, in part, by utilizing a third party database called "Bullhorn" to manage HPA's client lists, emails and other critical data. (Goel Decl., ¶5)

Goel, the founder and sole member of HPA, also operates personal Yahoo and professional LinkedIn accounts. Notably, Goel's log-in information for his Yahoo and LinkedIn accounts were stored on the HPA network server and Office365. (Goel Decl., ¶6; Declaration of Kevin Cohen ("Cohen Decl." ¶4)

B. <u>Plaintiffs Accounts Were Hacked.</u>

Plaintiffs recently discovered that HPA's Bullhorn account, client lists, consultant lists, executive professionals database, contacts information, Microsoft Office365 emails, and other private information and critical business data, along with Goel's personal Yahoo and professional LinkedIn accounts, have all been hacked by an unknown source. (Goel Decl., ¶7; Cohen Decl., ¶5)

As a result of these unauthorized accesses to HPA and Goel's private and critical information, an unknown and unauthorized source has obtained key, proprietary and confidential information and is in a position to cause irreparable harm to Goel and HPA's business, assuming that has not already occurred. (Goel Decl., ¶14; Cohen Decl., ¶12)

1. <u>Goel's Personal Yahoo and Professional LinkedIn Accounts were Illegally Hacked</u>

Plaintiffs recently discovered two (2) unidentified log-ins (October 29, 2014 and October 30, 2014) to Goel's Yahoo account, using Outlook Web Access. Outlook Web Access accesses email over any browser on any computer. (Goel Decl., ¶8; Cohen Decl., ¶6)

On December 5, 2014, Goel received an email from Yahoo noting an unauthorized attempt to log into his personal Yahoo account from Romania.

Subsequently, Goel learned of multiple recent log-ins to his Yahoo account from IP addresses based in Michigan, Texas, Missouri and New Jersey, places Goel never travelled to during the log-in times. These particular log-ins were traced back to LTM. Whoever accessed Goel’s Yahoo account had apparently purchased large blocks of IP addresses from a company providing "anonymous internet access & browsing" for a fee. The Doe Defendants are believed to be using LTM to disguise his or her access to Goel's Yahoo account. (Goel Decl., ¶9; Cohen Decl., ¶7)

Goel discovered an unauthorized log-in to his LinkedIn account tied to a company called “FDCServers.net,” an ISP in Chicago, Illinois from November, 2014, using Microsoft Internet Explorer. Goel was not in Chicago at that time, and has not used Internet Explorer for at least 5 years. (Goel Decl., ¶10; Cohen Decl., ¶8)

2. **Highpoints Electronic Communications and Other Information Were Illegally Accessed**

On December 9, 2014, HPA received a log-in data download from Bullhorn, the 3rd party database application used to manage client lists, emails and other data that is stored on the cloud. Plaintiffs thereby discovered two unauthorized log-ins into HPA’s Bullhorn account. Specifically, Plaintiffs learned that on December 4, 2014 and December 5, 2014, an anonymous LTM IP address using an IP address block, accessed HPA’s private data including, without limitation, HPA’s access codes to Bullhorn, contact information for HPA’s clients and professional network, using a current partner and former HPA employee’s Bullhorn account access. Plaintiffs verified that these accesses were unauthorized. In addition, HPA continues to receive data downloads from Bullhorn, including dates, times, IP addresses, pages viewed, evidencing recent unauthorized access to HPA’s private network data. (Goel Decl., ¶11; Cohen Decl., ¶8)

Plaintiffs are aware of additional unauthorized log-ins to HPA’s system through the FDCServers.net, including (1) a log-in on October 18, 2014 to Goel's HPA Bullhorn account just after midnight for 20 minutes randomly searching the HPA database and (2) several accesses wherein someone printed out pages like "HPA client list" and "HPA consultant list". (Goel Decl., ¶12)

Plaintiffs believe that HPA's network was compromised in such a way that changing email passwords may not end the threat of further unauthorized log-ins. Upon discovering the unauthorized access at HPA, HPA installed a "network sniffer" at its offices to record all traffic on the HPA computer network. The "network sniffer" revealed that two of HPA's machines have been compromised and are being accessed using the LTM IP addresses. (Goel Decl., ¶13; Cohen Decl., ¶9)

C. <u>The Complaint</u>.

On January 22, 2015, Plaintiffs filed the Complaint in this action against the unknown Doe Defendants asserting causes of action for (1) Unlawful Access to Stored Electronic Communications (18 U.S.C. § 2701); (2) Fraud and Related Activity In Connection with Computers (18 U.S.C. § 1030); and (3) Invasion of Privacy (California Constitution, Article I, § 13). (Declaration of Jesse Kaplan, "Kaplan Decl." ¶2)

It is beyond dispute that someone unlawfully hacked into Plaintiffs electronic communications and accessed private and confidential information. Once the source of the hacking is identified, liability should be a certainty so that Plaintiffs will prevail upon the causes of action within the Complaint.

Plaintiffs first cause of action properly alleges that Defendants violated 18 U.S.C.A. § 2701 by, among other things, unlawfully obtaining access to HPA's network, Bullhorn account and Goel's personal Yahoo and professional LinkedIn accounts. As defined by the statute, these accounts constitute electronic communication services and remote computing services, effecting interstate commerce, to which HPA and Goel are subscribers. (Complaint, ¶¶25-43)

Plaintiffs second cause of action alleges that HPA's network, Bullhorn account, Office365 account, and Goel's personal Yahoo and professional LinkedIn accounts constitute "computers," as defined by the statute, that were intentionally accessed by Defendants without authorization, causing losses and damages. (Complaint, ¶¶45-48)

Plaintiffs third cause of action alleges the Defendants unlawfully invaded Plaintiffs legally protected right of privacy. As set forth in this cause of action, Plaintiffs sensitive, confidential and proprietary information was maintained within the accounts that were hacked by the Defendants. Plaintiffs had a reasonable expectation of privacy in this information. Defendants violated Plaintiffs' privacy rights by accessing this information. (Complaint, ¶¶50-55)

D. **The Requested Discovery Is Needed to Identify the Defendants**.

As Plaintiffs cannot identify Defendants since the IP addresses used to access the accounts are anonymous, Plaintiffs were forced to name Defendants as "Does" in the Complaint and pursue service of the subpoenas attached to this Motion.

Microsoft, Bullhorn and LTM will not release the information necessary to identify Defendants without a subpoena.

Plaintiffs received limited logs from Microsoft, however the logs did not contain time stamps and other information needed to identify the Defendants. Microsoft's representative directed Plaintiffs to pursue further information through a subpoena to their legal department. (Cohen Decl., ¶¶11-12)

LTM's business is to hide the identity of individuals using the internet so that LTM makes it as difficult as possible to ascertain any information about those individuals. After conducting a diligent online search to find a way to contact LTM directly, Plaintiffs were unable to do so and the only way to ascertain the needed information from LTM is through a subpoena. (Cohen Decl., ¶13)

Plaintiffs requested documents from Bullhorn, however, Bullhorn is expected to produce a limited set of documents in response. A subpoena to Bullhorn is required to receive the full extent of documents that will implicate the entirety of hacking that is alleged in this matter. (Cohen Decl., ¶14)

Plaintiffs propose serving subpoenas to Microsoft, Bullhorn and LTM seeking the production of documents enabling Plaintiffs to identify the Defendants as the source of these unauthorized log-ins to Plaintiffs private accounts. (Kaplan Decl., Exs. 1-3). Plaintiffs' counsel has prepared these subpoenas and is ready to serve them on Microsoft, Bullhorn and LTM.

The subpoenas requested by this Motion are critical to determine the person and/or entity illegally accessing Plaintiffs electronic communications and other information. Plaintiffs expect the subpoenas will identify the source of the hacking at issue in this case, either by providing information identifying the Defendants or to subpoena other ISPs to get a step closer to locating the real perpetrator of the hacking. (Cohen Decl., ¶15)

In this case, Plaintiffs took all possible initial steps to identify the hacker(s) prior to commencing this action and seeking permission to serve these subpoenas. Those steps included (a) examining log files which lead to London Trust Media and unexplained use of closed accounts; (b) imaging and examining other computers and electronic media of Plaintiffs for additional logs or information; and (c) setting up a traffic sniffer to locate inappropriate traffic. At this point, service of these subpoenas is the only logical next step that can be taken to identify, or move closer to identifying, the hackers. (Cohen Decl., ¶16)

If the companies to which these subpoenas are addressed retain proper logs, there is a reasonable likelihood that Plaintiffs will be able to identify the Defendants through the user data, time stamps and other identifiable information from these logs. (Cohen Decl., ¶17)

If Plaintiffs are able to identify Defendants through the requested subpoenas, Plaintiffs intend to amend their Complaint to name the Defendants.

III. **GOOD CAUSE EXISTS TO ALLOW PLAINTIFFS TO PROPOUND DISCOVERY IN ORDER TO IDENTIFY THE DEFENDANTS.**

The Court may authorize expedited discovery before the Rule 26(f) meeting for good cause. *See Semitool, Inc. v. Tokyo Electron Am.*, 208 F.R.D. 273, 275 (N.D. Cal. 2002). A court order permitting early discovery may be appropriate "where the need for the discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *Semitool*, 208 F.R.D. at 276.

Good cause exists in the internet context when online defendants attempt to mask their identify thereby preventing plaintiffs from prosecuting their claims against internet tortfeasors. *See Liberty Media Holdings, LLC v. Doe*, 2010 U.S. Dist. LEXIS 116816, *3-4 (S.D. Cal. Nov. 3, 2010) (finding good cause to allow plaintiff to issue subpoenas to obtain the identity of Doe internet defendants). "[I]n light of the conflict between the need to provide injured parties with a forum in which they may seek redress for grievances, and the right to use the internet anonymously or pseudonymously, a few principles should apply to whether discovery to uncover the identity of a defendant is warranted." *Liberty Media Holdings*, 2010 U.S. Dist. LEXIS at *3-4.

Here, good cause exists to allow Plaintiffs to propound the proposed subpoenas on Microsoft, Bullhorn and LTM so that Plaintiffs can ascertain Defendants' identity. As already discussed, Plaintiffs cannot ascertain Defendants' identity without obtaining this information from these third parties. As a practical matter, unless Plaintiffs are permitted to obtain this information through expedited discovery, Plaintiffs cannot prosecute this matter and protect their private business and personal information. Plaintiffs would essentially be forced to dismiss this lawsuit. Conversely, there is no chance that either Defendants or third parties Microsoft, Bullhorn and LTM would be prejudiced by the requested subpoenas.

DATED: February 6, 2015

FREEDMAN + TAITLEMAN, LLP

By: __________________/s/__________________
MICHAEL A. TAITELMAN
JESSE KAPLAN
Attorneys for Plaintiffs
HIGHPOINT ASSOCIATES, LLC and
SUMEET GOEL